ADITEL news

LE JOURNAL D'INFORMATION DE L'ASSOCIATION ADITEL | #25 | FÉVRIER 2025

ON EN PARLE P.2
ZOOM P.4
SAVOIR-FAIRE & INNOVATION P.6
ADITEL & VOUS P. 14

LA PERTINENCE DU CONTINUUM

Édito de Didier Moreau, président d'Aditel

L'association de la sécurité publique et de la sécurité privée, ainsi que l'usage des nouvelles technologies, ont fortement participé au succès des derniers Jeux Olympiques et Paralympiques (JOP). Leur emploi en complémentarité a révélé qu'il était possible de faire face à des risques très importants. Face à la montée des violences et des incivilités partout sur le territoire, l'enjeu n'est pas le même. Toutefois, l'expérience acquise pendant ces JOP montre que les dispositifs de sécurité ne fonctionnent jamais aussi bien qu'en associant toutes les forces du continuum et les systèmes d'intelligence augmentée.

COMPLÉMENTARITÉS

L'IA révolutionne tous les jours la sécurité, ses solutions doivent être intégrées dans toute réflexion sur l'évolution du continuum. Notamment pour répondre à la majorité de Français qui se déclarent favorables à ces systèmes, selon une enquête d'Opinion Way. Cela pourrait faire l'objet d'une concertation entre les citoyens, les forces publiques et les grandes institutions, comme les banques... Quoi qu'il en soit, ces JOP laissent entrevoir de nouveaux débouchés pour le continuum. Cet événement qui a si fortement marqué l'année 2024 a créé un immense moment de joie, d'unité et de fierté pour la France. Aditel vous souhaite que de pareilles satisfactions emplissent votre vie professionnelle et personnelle en 2025.

Paris Fashion Week
2025
Modèle Continuum de sécurité

LES GRANDES TENDANCES DE LA SÉCURITÉ PHYSIQUE

Une étude réalisée dans le monde entier a interrogé les préoccupations et les priorités des professionnels de la sécurité physique, qu'ils soient utilisateurs finaux ou partenaires distributeurs. L'analyse des réponses, particulièrement dense, permet de se projeter sur les évolutions du secteur.

Entre le 12 août et le 15 septembre 2024, la société Genetec Inc. a mené une vaste enquête à l'échelle mondiale auprès des experts de la sécurité physique. L'état des lieux qui en résulte, après analyse d'un échantillon de 5696 personnes interrogées, est riche d'enseignements.
La note de synthèse de cette étude fait notamment apparaître que 48% des utilisateurs finaux en Europe considèrent l'obsolescence de leur système de sécurité physique et/ou de leur infrastructure informatique comme leur principal défi et que 66% des partenaires distributeurs déclarent que leurs clients veulent bénéficier de nouvelles technologies et fonctionnalités.
Dans le détail, 64% des utilisateurs finaux jugent le contrôle d'accès (43%) et la vidéosurveillance (42%) comme les fonctionnalités ou processus les plus importants. Ces statistiques corroborent le fait que 91% des activités des partenaires distributeurs ont porté sur l'un ou l'autre de ces systèmes centraux. Par ailleurs, 60% des utilisateurs finaux disent avoir déployé l'intégralité de leur système de sécurité physique sur site (sans recourir au cloud), et ils sont 77% à affirmer que les services de sécurité physique et de technologie de l'information travaillent en collaboration dans leur organisation.

> La majorité des utilisateurs finaux se préoccupent en priorité des contrôles d'accès et de la vidéosurveillance.

ATTRACTIVITÉ EN BERNE

Un sujet majeur de préoccupation, sur lequel se retrouvent utilisateurs finaux et partenaires, est la difficulté à recruter, et les perspectives pour 2025 ne vont pas dans le sens d'une amélioration. En effet, 72% des partenaires distributeurs s'attendent à ce que les problèmes de recrutement perdurent, tandis que 6% seulement pensent que la situation va s'améliorer. Logiquement, ils sont nombreux à craindre que ces pénuries de compétences aient un impact sur leurs projets, 44% d'entre eux estimant que le manque d'attractivité du secteur entraînera des retards en 2025.
Autre résultat intéressant, les utilisateurs finaux affirment que des raisons budgétaires liées aux « coûts du stockage en ligne, de conservation des données et de bande passante » ont influencé l'adoption des solutions cloud au sein de leur organisation.
« La peur de la perte de données et la question globale du contrôle » constituent la deuxième raison invoquée, ce qui montre que les professionnels de la sécurité physique cherchent à migrer progressivement leurs charges de travail vers le cloud, à un rythme adapté à leur entreprise.
Enfin, d'après l'étude, il y aurait une implication plus forte des services informatiques dans les décisions relatives à la sécurité physique. À la question « Quels services prennent part aux décisions d'achat ? », les personnes interrogées ont constamment placé les services informatiques au-dessus des services de sécurité physique.

COMMENT L'IA RISQUE DE CHANGER LA DONNE DES ASSURANCES

Avec la généralisation des usages de l'intelligence artificielle, le secteur de l'assurance entre lui aussi dans un nouveau monde. La définition des responsabilités et l'évaluation des risques se trouvent transformées par les nouvelles technologies.

Dans l'Argus de l'assurance, deux experts évoquent la transformation de la couverture et de la gestion des risques à l'ère de l'intelligence artificielle. Les risques liés à l'utilisation de l'IA dans notre quotidien, s'ils sont loin d'être établis, nécessitent de réfléchir à l'évolution des contrats.
Les compagnies d'assurance doivent d'abord identifier ces risques spécifiques, tels que les erreurs algorithmiques, les failles de sécurité, les biais des données ou les risques liés des prises de décision automatisées.
Le sujet est tellement complexe qu'il peut réduire la capacité des assureurs à prendre des décisions sans assistance technologique. En cas de dysfonctionnement des systèmes, il deviendrait difficile de déterminer les responsabilités. Les contrats devront les préciser, ainsi que les recours disponibles pour les clients utilisateurs, même si les décisions prises par l'IA peuvent être difficiles à expliquer.
Il sera peut-être nécessaire de développer des assurances spécifiques pour les développeurs d'algorithmes d'IA ou pour les entreprises utilisant ces systèmes. Les contrats devront aussi intégrer des méthodes d'évaluation des risques tenant compte de la rapidité d'évolution des technologies.
Cela nécessitera l'utilisation de l'IA elle-même pour évaluer les risques en temps réel et ajuster les primes et les couvertures en conséquence. Les assureurs devront aussi collaborer avec des experts en IA, des entreprises technologiques et des régulateurs pour comprendre les évolutions légales et normatives, et pour s'assurer que les contrats sont conformes aux nouvelles régulations. Enfin, ils devront inclure des efforts pour sensibiliser les assurés à l'utilisation responsable de l'IA et aux possibilités qu'offre l'assurance en cas de problème.

PÉNURIE

76% Les trois quarts des distributeurs du secteur de la sécurité physique disent avoir du mal à recruter des techniciens en installation.
Source : État de la sécurité physique 2025 - Genetec

RISQUE

Les incendies liés aux batteries lithium-ion utilisées dans les voitures, les trottinettes et les vélos électriques, les téléphones mobiles ou encore les ordinateurs sont scrutés de près par les assureurs. En effet, le développement très rapide de cette technologie génère des problématiques variées en termes de prévention du risque. C'est pour cette raison que France Assureurs et Assurance Prévention ont confié en 2024 au CNPP la réalisation d'une campagne d'essais qui prolonge l'étude lancée en 2022 par le CNPP sur le stockage des batteries.

CYBERSÉCURITÉ

« Entrée en vigueur le 17 octobre dernier, la directive NIS2 avait pour objectif d'amener une conformité en matière de sécurité pour l'ensemble de l'Union Européenne. Mais force est de constater que seulement six pays ont intégré NIS2 dans leur législation. » Cette nouvelle règle européenne vise à renforcer le niveau de sécurité des systèmes d'information.
Source : Nicolas Lacourte, Solution Manager cybersécurité chez NXO

Le continuum de sécurité en débat

La réussite sécuritaire des Jeux Olympiques 2024 a montré l'intérêt de favoriser les complémentarités entre sécurité publique et privée et de s'appuyer sur les nouvelles technologies. Une expérimentation concluante, alors que les freins réglementaires demeurent.

Le succès des Jeux Olympiques et Paralympiques (JOP) de Paris sur le plan sécuritaire est à mettre en grande partie au crédit du continuum de sécurité, qui a permis de disposer des ressources humaines, matérielles et technologiques nécessaires pour faire face aux diverses menaces. La collaboration entre forces de sécurité intérieure et sécurité privée, mais aussi les moyens technologiques déployés, ont rendu possible l'atteinte des objectifs fixés. Alors que ces JOP ont été l'occasion d'expérimenter de nouvelles technologies de sécurité, une enquête du Continuum Lab, think-tank des métiers de la sécurité et de la justice, révèle que 87 % des Français sont favorables à l'utilisation de la vidéoprotection dans les espaces publics (41 % se disant tout à fait favorables). 76 % des personnes interrogées estiment également que la vidéoprotection contribue directement à la résolution des enquêtes.

ACCEPTATION CITOYENNE

Les réponses indiquent la bonne acceptation globale de cette technologie : 65 % des Français considèrent ainsi l'IA comme un outil utile pour les forces de sécurité, là où 33 % expriment des préoccupations quant à son impact potentiel sur les libertés individuelles. Cette question de l'atteinte aux libertés rend complexe la généralisation de l'usage de ces nouvelles technologies, que ce soit dans le domaine public ou dans les espaces privés, comme l'a illustré la loi relative aux Jeux Olympiques et Paralympiques, qui a souhaité encadrer les dispositifs mis en place. Pourtant, on se rend compte que les enjeux sécuritaires des banques concernent aujourd'hui davantage des problèmes comportementaux comme les incivilités que le détournement de cash. Alors que des solutions opérationnelles basées sur l'IA voient le jour pour y répondre, il est fondamental d'établir rapidement un cadre légal pour pourvoir en bénéficier.

L'introduction des solutions basées sur l'IA nécessite la définition rapide d'un cadre légal pour leur utilisation.

Précurseur

Cela fait déjà 7 ans que les députés Alice Thourot et Jean-Michel Fauvergue ont formulé leurs 78 propositions pour un continuum de sécurité. Le rapport issu de leur mission parlementaire préconisait notamment d'inclure les sociétés de formation à la sécurité dans les instances de contrôle de la sécurité privée et de mettre en place un encadrement strict des règles de sous-traitance. Il proposait également de transférer à des sociétés privées des missions non régaliennes actuellement assurées par les forces de sécurité de l'Etat.

La vision d'un expert

Après une mise en place informelle, par le bas, en réponse à des événements ponctuels, la coopération public-privé sur la sécurité doit être normalisée, estime Guillaume Farde, maître de conférences à Sciences Po.

Auteur d'un ouvrage remarqué sur le sujet (Le continuum de sécurité nationale. Quelles externalisations pour demain, éditions Hermann), l'universitaire Guillaume Farde en a ainsi évoqué les enjeux lors d'une conférence chez Preventica : « Le continuum de sécurité, c'est l'idée que l'Etat et les forces de sécurité intérieure de l'Etat ne seraient plus les seuls aujourd'hui à pouvoir assurer les missions de sécurité intérieure, et qu'ils partageraient ces missions avec d'autres, ces autres étant les polices municipales et la sécurité privée. De ce fait, la sécurité privée et les polices municipales se sont développées en France au point qu'on leur a confié progressivement, dans le temps long de l'histoire, un nombre de missions qui autrefois étaient assurées par les forces de police et les forces de gendarmerie exclusivement.

Les attentats de 2015 et les manifestations des gilets jaunes ont beaucoup accéléré la coopération entre secteur public et secteur privé. Les problématiques d'ordre public qui se sont posées à cette occasion ont entraîné des modes de coopération assez inédits. Chaque vendredi, le préfet de police de Paris recevait les représentants de la sécurité privée et les directeurs sûreté des entreprises pour partager l'information sur les manifestations à venir. Ensuite, pendant les manifestations, les acteurs publics et privés partageaient aussi leurs informations dans le but d'améliorer la sécurité des personnes et des biens. Cette coopération public-privé, qui a continué pendant les JO, est aujourd'hui informelle. Elle s'est faite par le bas, par la base, à la faveur des événements et des difficultés qui ont pu se présenter. Le défi qui se pose à présent, c'est celui de la normalisation de cette coopération. Il va falloir la formaliser pour pouvoir l'inscrire dans le temps long. » Cet enjeu constituera un nouveau chantier pour les banques qui doivent veiller à ce que cette formalisation ne soit pas un frein aux nouvelles technologies.

Sotel, une offre adaptée en surveillance humaine

Marie-Isabelle Salmeron-Santi, membre du directoire de Sotel, détaille la vision stratégique et opérationnelle de l'entreprise pour répondre aux évolutions des besoins de ses clients du secteur bancaire.

« La banque est notre ADN, et nous adaptons au mieux nos services aux besoins spécifiques de nos actionnaires et clients. Notre politique en matière de surveillance humaine s'appuie sur les exigences fortes que nous avons identifiées. En premier lieu, la gestion des moyens d'accès est un élément essentiel de notre prestation. Ainsi, tous les moyens d'accès sont enregistrés et suivis dans un logiciel développé par nos soins, afin d'assurer la meilleure traçabilité, et les procédures en place permettent une anonymisation totale des moyens d'accès confiés.

RÉACTIVITÉ ET CONFORMITÉ

Par ailleurs, les banques ont des besoins divers en surveillance humaine. Il ne s'agit pas uniquement d'intervenir sur alarme ou de mettre en place des mesures conservatoires. Il faut également être réactif sur des demandes particulières, comme la sécurisation du personnel face aux cas d'incivilité forte, ou disposer d'agents en nombre suffisant pour des événements particuliers, comme récemment le passage de la flamme olympique. Tout le territoire est couvert grâce à un réseau de partenaires référencés, dont nous contrôlons régulièrement la conformité. Nous avons également développé un logiciel pour le suivi rigoureux et complet des prestations : planification, contrôle systématique et anticipé des prises de service, vérification des appels de sécurité, autorisation pour le départ, enregistrement de toute non-conformité (par exemple, intervention sans moyens d'accès). Toutes les actions sont enregistrées et horodatées en main courante. L'intégration de bordereaux de prix clients exhaustifs permet d'établir une facturation juste des prestations. Et la création d'une application mobile complémentaire optimise encore les échanges avec les agents sur site.

> « Notre politique en matière de surveillance humaine s'appuie sur les exigences fortes que nous avons identifiées chez nos clients du secteur bancaire. »

PRESTATION SPÉCIFIQUE

Grâce à cet outil, nous assurons également le suivi opérationnel et la préfacturation des prestations pour le compte de clients qui ont contractualisé avec différents acteurs du marché, mais qui ont souhaité confier toute la gestion des demandes et le pilotage opérationnel à Sotel. La préfacturation intègre également les éventuelles pénalités contractuelles liées aux non-conformités. Cette prestation très spécifique, appelée "PFPO", contribue à renforcer la qualité des prestations, avec une diminution sensible des coûts. Elle apporte une aide précieuse aux responsables sécurité soucieux de leur budget en surveillance humaine. Enfin, le besoin de reporting des clients n'a pas été oublié. L'année 2025 verra évoluer le serveur extranet afin de fournir de meilleurs outils de pilotage. En surveillance humaine comme pour toutes les activités du groupe, Sotel cherche en permanence à évoluer pour apporter le meilleur service. »

La solution digitale d'Azursoft dédiée à la gestion des incivilités

VIGI-Tools© s'ajoute à la gamme proposée par le fournisseur en matière de prévention des risques. Elle offre aux entreprises et à leurs collaborateurs une interface simple d'utilisation pour le signalement, le suivi et le traitement des incivilités.

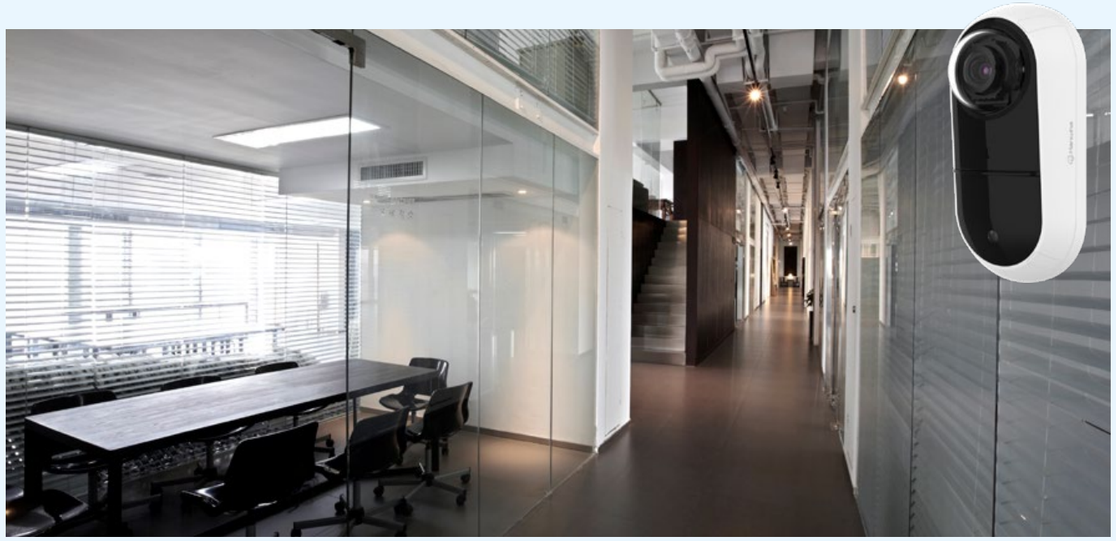
Dans une société où les incivilités et les agressions verbales ou physiques de la part d'interlocuteurs externes à l'entreprise (clients, prestataires…) deviennent malheureusement de plus en plus fréquentes, il est essentiel pour l'employeur de mettre en place une stratégie de prévention. C'est l'intérêt d'Alfatea©, logiciel HSE intégré, développé par AzurSoft, qui couvre l'ensemble des outils nécessaires aux professionnels de la prévention des risques : évaluation des risques ; document unique ; accidents du travail ; plans d'actions ; audits ; plans de prévention ; protocole de sécurité ; permis de feu ; vérifications périodiques ; formations ; habilitations ; fiches de poste ; maladies professionnelles ; événements indésirables ; indicateurs et tableaux de bord.

> « Les entreprises utilisatrices peuvent anticiper les incidents, mesurer leurs impacts et contribuer à la santé et à la sécurité des salariés. »

PRÉVENTION GLOBALE

La solution VIGI-Tools©, dédiée à la gestion de incivilités, s'inscrit dans ce processus de prévention. Elle donne la possibilité à tous les collaborateurs d'une entreprise de signaler une incivilité sur une interface simple et accessible à tous, déclenchant des workflows de traitement immédiat pour certains, différé pour d'autres. L'entreprise peut intégrer ces événements dans son système global de prévention, avec des fonctionnalités de suivi, de traçabilité, d'analyse des causes, etc. « Les collaborateurs sont assurés que ces situations sont prises en compte, et traitées, car ils peuvent suivre leurs signalements à tout moment », précise AzurSoft. En intégrant les principes de prévention des incivilités dans une approche digitale, les entreprises utilisatrices peuvent ainsi anticiper les incidents, mesurer leurs impacts et mettre en œuvre un plan d'actions pour la santé et la sécurité des salariés. La solution est en cours de déploiement par le groupe BPCE. « Elle nous permettra d'optimiser et d'homogénéiser les pratiques de prévention, d'accompagnement des victimes et d'analyse et de suivi des événements », explique Dominique Colson, responsable projets sécurité du groupe BPCE.
Une formation innovante, un guide managérial de bonnes pratiques, un logiciel de déclaration Alfatea©, un bouton d'alerte numérique et un accompagnement juridique ont été mis en place en s'appuyant sur les pratiques mises en œuvre par les acteurs de terrain.

Hanwha Vision place sa caméra intelligente à hauteur d'homme



Le fournisseur propose un dispositif de surveillance basé sur l'IA qui renforce les capacités d'identification des risques et d'alerte, particulièrement adapté à l'environnement des agences bancaires.

La caméra IA murale TNV-C8011RW de Hanwha Vision répond aux contraintes du secteur bancaire. Conçue pour capturer des détails précis à hauteur d'œil, elle améliore les dispositifs de surveillance des entrées et sorties des agences, renforçant la sécurité et réduisant les erreurs grâce à des fonctionnalités d'IA avancées. Sa capacité à opérer dans des conditions d'éclairage variables et sa résistance au vandalisme la rendent fiable dans des environnements exigeants tels que les banques et institutions financières. Contrairement aux caméras classiques, qui offrent généralement une vue de haut en bas, la TNV-C8011RW s'installe à hauteur humaine, au niveau des yeux. Cela rend possible une vue claire des visages, même lorsque les individus filmés portent des chapeaux ou utilisent des parapluies.

La solution rend possible une vue claire des visages, même lorsque les individus portent un chapeau ou utilisent un parapluie.

VISION À 180°

L'objectif panoramique de la caméra offre un champ de vision de près de 180 degrés, avec une inclinaison ajustable à plus ou moins 25 degrés pour éviter les angles morts. La résolution 5 Mpx assure quant à elle la capture de tous les détails requis pour identifier des personnes – améliorant ainsi à la fois la sécurité et l'expérience utilisateur. La fonctionnalité infrarouge (IR), avec sa portée de 15 mètres, génère des images claires en conditions d'éclairage variables. En complément, la TNV-C8011RW intègre une fonctionnalité de prise de son avancée, permettant à l'agent bancaire, si besoin, d'être écouté en temps réel au sein de son agence ou par un télésurveilleur en cas d'urgence. Dès qu'un bouton « panique » est activé, le système transmet automatiquement l'audio, facilitant une intervention rapide.

Anticipation

« Grâce à l'IA, les systèmes vidéo formés sur la base de scénarios réels définis par les utilisateurs seront en mesure de prédire certains comportements et d'alerter les opérateurs d'éventuels risques d'incidents avant même qu'ils ne se produisent. »
John Lutz Boorman, responsable des produits et du marketing chez Hanwha Vision Europe.

Lanaccess : des caméras « augmentées » conformes à la réglementation

Alors que les pouvoirs publics cherchent un difficile équilibre entre sécurité et protection des libertés individuelles, le récent règlement européen propose une approche graduelle intéressante pour la régulation des dispositifs d'IA. Une évolution qui pourrait clarifier les règles en vigueur.

La réglementation européenne sur la protection des données, l'une des plus strictes au monde, n'interdit pas une grande partie des applications d'intelligence artificielle dans le domaine de la sécurité. Néanmoins en France, la Loi Informatique et Libertés restreint la plupart de ces applications. Le concept de caméras « augmentées » ou « algorithmiques », utilisé par la CNIL, englobe des applications très diverses. Il est essentiel d'analyser ces applications afin de mieux comprendre les risques et de fixer des conditions d'utilisation spécifiques. Les caméras dites « biométriques » utilisent des données sensibles pour la vie privée « aux fins d'identifier une personne physique de manière unique » par la reconnaissance faciale. Le traitement de ces « catégories particulières de données » est interdit, sauf si « la personne concernée a donné son consentement explicite» et si « le traitement est nécessaire pour des motifs d'intérêt public importants ». Mais ces deux exceptions sont difficiles à satisfaire. En pratique, l'usage des caméras « biométriques » reste interdit dans tous les pays de l'UE pour la seconde exception.

Il est essentiel d'analyser les applications d'IA afin de mieux comprendre les risques et de fixer des conditions d'utilisation spécifiques.

En France, ce sont non seulement les caméras « biométriques », mais également les caméras « augmentées », qui sont interdites par défaut. Malgré ces restrictions, des milliers de caméras « augmentées » sont installées, jugées illégales par la CNIL. La question est de savoir où commence réellement le « traitement de données » : depuis les années 2000 des vidéosensors « avancés » utilisent l'analyse vidéo par soustraction de fond, et l'intelligence artificielle a considérablement amélioré ces fonctions. Quand une caméra doit-elle être qualifiée d'« augmentée » ?

AFFINER LES CATÉGORIES

Une approche intéressante est proposée par le Règlement européen 2024/1689, qui classe les pratiques liées à l'IA en plusieurs catégories :
- A haut risque pour certaines caméras « biométriques », soumises à des conditions strictes ;
- Avec obligation de transparence : autorisées sous conditions ;
- A risque minimal : autorisées sans restriction.

Le débat reste ouvert. Pour mieux protéger les individus et les biens, il est crucial de clarifier la réglementation et de recentrer le débat sur les caméras « biométriques ». En effet, si l'on doit localiser un terroriste pour prévenir un attentat, il est souhaitable que les forces de l'ordre disposent des meilleures ressources, tout en garantissant les droits des citoyens. Lanaccess propose, pour le métier bancaire et déjà en exploitation en France, des enregistreurs et des solutions vidéo équipées de caméras « augmentées » et intègre également des caméras « biométriques ».
« Nous sommes prêts à offrir des applications conformes à la réglementation actuelle et à évoluer avec le client vers les solutions de demain », explique la société.

A 40 ans, la certification A2P de CNPP reste la référence

Reconnue en France et à l'international, cette marque de qualité apporte aux professionnels et aux particuliers une garantie de fiabilité de leurs produits et systèmes de protection, qui a su s'adapter aux évolutions technologiques.

En 2024, CNPP a célébré le 40e anniversaire de sa marque emblématique A2P. En moins d'un demi-siècle, cette certification est devenue une référence incontournable pour les produits liés à la protection contre les intrusions et les incendies. La certification A2P atteste que les produits analysés répondent à des spécifications techniques définies (générales, niveaux d'accessibilité, conception et réalisation) et que leur qualité de fabrication est maîtrisée. Elle est délivrée à l'issue d'un processus qui comprend des essais en laboratoire et un audit du ou des sites de fabrication. Des contrôles périodiques sont effectués pour le maintien de la certification. Il s'agit donc d'une reconnaissance de la performance et de la fiabilité des produits, la garantie d'une qualité reconnue par les professionnels de la sécurité.

PRESCRITE PAR LES ASSUREURS

La certification A2P concerne les blocs-portes, les serrures de bâtiment, les fenêtres et fermetures de bâtiment, les coffres-forts, les serrures de coffre, les systèmes de neutralisation des billets, les équipements d'enceinte technique de sécurité, les armoires sprinkleurs et les systèmes d'extinction automatique à gaz.
Elle s'applique également, à travers une certification conjointe délivrée avec AFNOR Certification, aux centrales d'alarme et transmetteurs téléphoniques, détecteurs (infrarouge, chocs, ouverture à contact, mouvement, etc.), dispositifs d'avertissement sonore, lumineux à éclats, alimentations, boîtes de dérivation, organes intermédiaires et dispositifs générateurs de brouillard. Aujourd'hui, cette certification reconnue en France et à l'international est prescrite par la profession de l'assurance.
Les produits certifiés A2P sont utilisés dans des contextes variés, allant des résidences privées aux sites industriels sensibles, en passant par les bâtiments publics. Ce succès dans la durée doit beaucoup à l'investissement constant des équipes de CNPP pour que le label reste pertinent, selon Guillaume Savornin, directeur général du groupe : « Depuis 40 ans, la certification A2P évolue pour répondre aux défis posés par les avancées technologiques et les nouvelles formes de criminalité. Les critères d'évaluation sont continuellement mis à jour pour inclure les dernières innovations en matière de sécurité, comme les systèmes de verrouillage électronique et les nouvelles technologies en matière de détection. Nos équipes travaillent sans relâche à créer un environnement de confiance, ils proposent aux particuliers comme aux entreprises des repères pour choisir des équipements de sécurité de qualité. Je me réjouis de célébrer cet anniversaire. »

> Le maintien de la certification après des essais en laboratoire et l'audit des sites de production nécessite la réalisation de contrôles périodiques.

Ferrimax : une conformité garantie de la fabrication à l'installation

Utiliser des produits certifiés est nécessaire, mais pas suffisant s'ils ne sont pas installés correctement. D'où l'intérêt de faire réaliser un audit d'installation comme ceux que propose le fabricant de coffres-forts Ferrimax.

« Avant de fabriquer et commercialiser des enceintes techniques de sécurité (ETS), les industriels doivent se soumettre à des normes, référentiels et tests de conformité de leurs produits. Mais après la sortie de l'usine, il reste plusieurs maillons faibles. S'ils n'ont pas été identifiés et anticipés, les failles s'installent, les vices cachés apparaissent et c'est la non-conformité de l'installation qui nous attend », explique Antonio de la Casa, CEO de Ferrimax et membre du comité A2P et du Syfraco. En effet, le processus de validation du CNPP pour apposer la marque A2P ne comprend pas la vérification de l'installation, et rien ne garantit que l'installateur respecte les méthodologies préconisées par le fabricant qui a été certifié.

> C'est quand l'installateur prend des initiatives pour combler les écarts que risquent d'apparaître des non-conformités.

VISITES DE VALIDATION

L'installateur n'étant pas forcément le fabricant, il faut s'assurer de la validité des informations communiquées en avant-projet. La prise de cotes nécessite impérativement un curage complet du site. Il faudra aussi tenir compte des éléments à intégrer (automates, portes blindées, boîtes aux lettres, coffres de transfert, consignes, etc.), mais également des passages de câbles, comme de la ventilation, de manière à préserver les réservations validées par le CNPP.

Un chantier étant en constante évolution, plusieurs visites sont nécessaires pour la validation de l'étude de réalisation. Si des écarts sont constatés au cours de l'installation, l'installateur est tenté de prendre des initiatives. C'est alors que risquent d'apparaître des non-conformités : découpage des panneaux pour les redimensionner, agrandissement des réservations, modifications et ajouts de passages de câbles, diamètre non respecté pour la VMC, chevilles de fixation non conformes aux préconisations du fabricant.
La solution idéale est un audit externe réalisé en cours et en fin de montage pour certifier l'adéquation entre le dossier technique et la réalisation.
La solution intermédiaire serait d'exiger du fabricant un dossier technique d'installation avec des instructions précises, un DOE (dossier d'ouvrage exécuté) complet ainsi qu'un certificat de conformité de montage de la part de l'installateur.
Le problème étant identifié, c'est aux acteurs impliqués dans le projet de prendre conscience des risques.

Ferrica, l'expert de la maculation des billets

La solution Smartstain continue à protéger les distributeurs bancaires contre les tentatives d'attaque. Affinée depuis son premier déploiement, elle constitue aujourd'hui le cœur d'une suite logicielle alliant temps réel, précision et fiabilité.

Lors de l'introduction de l'euro, en 2002, Ferrica présentait une solution intelligente pour prévenir les attaques des DAB. Smartstain est un système de projection d'encre sur les billets contenus dans les deux à quatre cassettes du DAB qui se déclenche lorsqu'il détecte une attaque ou une tentative de vol. Plus de 20 ans après, la solution équipe plus de 20 000 distributeurs dans le monde. Sa mémoire embarquée inscrit au fil de l'eau près de 36 000 événements. Grâce à l'analyse de cet historique, il est possible de reconstituer le détail d'un événement ou d'une attaque (quel capteur, combien de temps, dans quel ordre, heure et cause de maculation…) et de définir des preuves, utilisées dans l'investigation judiciaire. Un décret de 2014 du ministère de l'Intérieur impose d'ailleurs à tous les acteurs du maniement des espèces et aux banques de sécuriser les flux d'argent en insérant un système de maculation de billets. Ferrica a ajouté un traceur à code unique ADN dans toutes les cassettes. Les billets volés maculés d'encre et l'analyse de l'ADN par les laboratoires de police et de gendarmerie font ainsi le lien entre le butin, les conditions d'attaque et les auteurs. Smartstain constitue le cœur d'une suite logicielle, matérielle et fonctionnelle qui entrave les tentatives de vol et restitue les informations.

La complémentarité entre le superviseur Observer et la suite On-Smart apporte une aide précieuse aux responsables sécurité des sites bancaires exposés aux attaques.

OPTIMISATION

La complémentarité entre le superviseur Observer et la suite On-Smart apporte une aide précieuse aux responsables sûreté et sécurité des sites bancaires exposés aux attaques : On-Smart combine le suivi GPS en temps réel et la surveillance de la liaison avec la gestion centralisée du serveur. Le cryptage des données et l'accès via un navigateur garantissent une sécurité élevée. Le module GSM/GPRS de Smartstain Observer assure des transmissions cryptées, rapides, fiables, indépendantes et sécurisées vers le serveur central. Observer indique automatiquement l'état de la cassette et le suivi du numéro de série, éliminant les retranscriptions et les efforts manuels des personnels sans perdre la précision. Les tournées de maintenance sont optimisées par une suggestion intuitive.
La solution s'installe rapidement sur n'importe quel coffre-fort en première monte ou en activité, évitant les interventions physiques fastidieuses et offre immédiatement des communications indépendantes et cryptées. Aujourd'hui, avec Ferrica, il est devenu classique d'être prévenu par SMS d'une faiblesse technique détectée ou d'une attaque en cours… sur un DAB installé parmi un parc important de machines en service !

Registre Sécurité dématérialise les obligations réglementaires dans le bâtiment

Cette application a pour objectif de simplifier la gestion et le suivi de la sécurité des bâtiments. Elle offre aux utilisateurs une solution optimisée pour piloter les interventions à distance et centraliser l'information.

L'outil donne en quelques clics une vue précise sur les mesures mises en place pour assurer la sécurité du bâtiment.

Professionnel du secteur de la sécurité depuis quelques années, Jérôme Périgord a créé une solution pour relier la sécurité des bâtiments à la gestion administrative, sans que cela devienne une charge trop importante. En 2012, ce passionné d'informatique imagine un outil permettant la dématérialisation des registres de sécurité, et achète le nom de domaine qui correspond à cette nouvelle activité. Rejoint par Stéphane Guyon, il lance *registresecurite.com*.
En 2019, les deux associés démarrent le développement d'une solution full web, accessible à tous. Leur but : simplifier la gestion des obligations réglementaires, et gérer et piloter à distance pour éviter des déplacements.
L'application apporte un ensemble de fonctionnalités très intéressantes :

- suivre les non-conformités déclarées par les prestataires et assurer le suivi jusqu'à la résolution définitive ;
- générer une synthèse à partir des éléments récoltés automatiquement pour les présenter aux autorités compétentes ;
- suivre l'ensemble des formations du personnel, gérer les attestations de suivi des formations et télécharger le passeport de prévention de chaque salarié si nécessaire.

Elle facilite en outre le partage des informations avec les collaborateurs, les intervenants et les autorités compétentes.

PERSONNALISATION

L'application planifie aussi les contrôles de sécurité et les visites techniques, envoie les dates de missions à réaliser pour les interventions des prestataires avec une relance automatique. Enfin, elle permet de créer un tableau de bord de manière totalement personnalisée, donnant accès en quelques clics à une vue globale de l'état des sites. Toutes les entreprises de type industriel, commercial, de services, les établissements publics ou privés, les bâtiments d'habitation ou encore les lieux de travail ont l'obligation de tenir à jour un registre de sécurité. L'objectif étant d'évaluer les risques pour élaborer et mettre en œuvre des plans d'action dans le but d'améliorer la sécurité. L'outil créé par Registre Sécurité permet en quelques clics d'avoir une vue précise sur les mesures mises en place pour assurer la sécurité des bâtiments. Il augmente ainsi la productivité du responsable sécurité en lui faisant gagner un temps précieux.

Fiamma Luzzati, le crayon bien affûté d'AditelNews

Vous connaissez ses dessins qui croquent avec talent et sur un ton décalé les articles de votre newsletter. Sicilienne d'origine, parisienne de cœur, Fiamma Luzzati a été économiste et historienne de l'art, avant de bifurquer vers la bande dessinée autobiographique sur le blog de Libération. Eclectique, la dessinatrice et scénariste aime se lancer des défis aussi divers qu'animer une BD scientifique pour Le Monde, dans laquelle elle scénarise des entretiens avec des experts, ou adapter un roman d'Alexandre Dumas, son projet du moment.

Dernièrement, elle a publié un livre remarqué, « L'emprise, histoire d'une manipulation », paru chez Dunod Graphic en 2024.

L'AVANTAGE DE L'APPLI "MAKE-UP GENIUS SUR VOS COPINES, C'EST QU'ELLE VOUS DONNE DES CONSEILS SANS L'ARRIÈRE PENSÉE DE VOUS PIQUER VOTRE MEC.

METTONS TOUT DE SUITE LES CHOSES AU CLAIR : JE N'ENVISAGE AUCUNE POSSIBILITÉ DE RELATION INTIME AVEC UN HOMME QUI MANGE DES TAGLIATELLE AU BEURRE ET DU FAUX FILET À LA MOUTARDE DANS LA MÊME ASSIETTE.

Votre association

Aditel a pour objet de favoriser les échanges d'expériences entre les membres de l'association, de mener des actions communes avec les instances bancaires nationales auprès des assureurs, des constructeurs et des pouvoirs publics.

L'association se compose de membres actifs, personnes morales, représentantes des banques ou des télésurveilleurs dont le capital est détenu majoritairement par les établissements de crédit.

Les cotisations offrent la possibilité de participer gratuitement au forum qui se déroule chaque année dans une ville différente et de se tenir informé de l'actualité, dans le domaine de la sécurité, grâce à trois newsletters par an.

FORUM 2025

Le 34e Forum d'Aditel se déroulera les 25 et 26 septembre à Rennes.

RÉSEAUX SOCIAUX

Aditel, c'est aussi une communauté présente sur les réseaux sociaux. Vous pouvez suivre l'actualité de l'association sur notre compte LinkedIn : **https://www.linkedin.com/company/aditel-association/**

AditelNews est édité par l'association Aditel : BP 31012 - 54521 Laxou Cedex • Comité de rédaction : Didier Moreau, Claude Pace • Rédaction : Exergue • Direction artistique & mise en pages : Alexandra Pourcellié, Arekusu • Illustrations : Fiamma Luzzati • Photos : Istock (hors mention) • Contact : contact@aditel-asso.fr